Protecting Personal Information at Fermilab: Advanced Course

Irwin Gaines – Lab Privacy Committee Chair

What You Will Learn

- Basic training
  - Why must we protect personal information?
  - What are the laboratory policies governing personal information
  - What is Protected Personally Identifiable Information (Protected PII)?
  - What are my obligations?
  - Where do I go if I have any question
- Advanced training
  - What are the special restrictions for those who must deal with PII (what are the exceptions to the basic rules)

Basic Training

Why do we need to protect personal information?

- ☞ Identity theft based on improper disclosure of personal information is a serious problem
- ☞ Several government agencies have been embarrassed by losses of large quantities of personal data
- ☞ Orders from White House --> DOE --> Office of Science mandate more careful treatment of personal information
- ☞ Fermilab respects the privacy of employees and users

Laboratory Policies on Personal Information

- We have lab policy and procedures:

1) Lab Policy (Director’s Policy Manual): Director's Policy Manual section 38.000
2) Lab Procedures:

   PII Procedures

Kinds of Personal Information

- PII (Personally identifiable information) is any information that specifically identifies an individual; not all needs to be protected
- “Protected” PII is PII that has a significant risk of identity theft if improperly disclosed (such as social security numbers; full definition on next slide)
- “Laboratory” PII is PII collected and maintained by Fermilab (not your own data: if you keep your personal credit card number on your computer it may be bad practice but is not in violation of lab policy). Much but not all Laboratory PII is Protected PII.

- These rules apply to electronic versions of Laboratory Protected PII

What is Protected PII?

- At Fermilab, Protected PII is defined as an individual’s name in combination with one or more of the following items:
  - social security number or foreign national ID number
  - passport number or visa number
  - driver’s license number
  - personal credit card number
  - bank account number
  - date and place of birth (both together, not one by itself)
  - mother’s maiden name
  - security clearance information
  - biometric information (fingerprints, retinal scan, DNA)
  - criminal records
  - detailed personal financial information (not merely salary history)
  - detailed medical records
  - detailed educational transcripts (not merely a list of degrees)

Your Obligations

- You must not have any Laboratory Protected PII on any of your computers
- You will need to sign a statement that you will inspect your computers and delete any Laboratory Protected PII you discovered (as part of this training)

- “Your computer” means any computer that you are the sole user of, and any file space you have on shared systems or servers. System administrators will NOT examine users’ files; this is the responsibility if each user.
- Note: this applies only to PII that “belongs” to Fermilab (PII that Fermilab collects and maintains, not your own information), and only to electronic copies of PII
- These rules apply to all computers, personally or laboratory owned, connected to laboratory networks.

Examples of PII that must be deleted

- Resumes or transcripts containing social security numbers or other Protected PII
- Conference databases with credit card numbers or visa numbers
- Spreadsheets with credit card or passport numbers of division/section travelers
- Word documents of trip reports or foreign travel forms containing passport numbers or other Protected PII

- Note that it is OK to enter Protected PII into external databases (like FTMS for foreign travel) as long as no local copies of reports containing things like passport numbers are kept on your computer.

What if I need to access PII

- The laboratory does have a need to maintain and process some PII (employee records, financial transactions) that a small number of employees need to access.
- If you are one of these employees you will receive “advanced” PII training to learn how to properly access this PII
- For further information contact your division/section PII representative (next slide)

Division/Section Privacy Reps

- AD: Tom Kroc
- CD: Irwin Gaines
- ND: Stephanie Schuler
- PPD: Luz Jaquez
- TD: Roger Slisz
- ESH&Q: Bill Flaherty
- ESH&Q: Jody Federwitz
- FESS: Odarka Jurkiw
- FIN: Mike Rosier
- WDRS: Heather Sidman

Advanced Training

Advanced Course

- For lab employees or users who need to access the small amount of protected PII the lab maintains
- DOE orders mandate:
  - Protected PII can only be kept in moderate level Major Applications
  - Protected PII cannot be downloaded to portable devices or devices outside the boundary of the major application
  - Any such downloads require a waiver from the DOE site manager, must be renewed every 90 days, and the data must be encrypted
  - Any remote access to protected PII required two factor authentication and a 30-minute timeout
  - Any suspected loss of PII must be reported to DOE within 1 hour (so we need to report to CIAC in 45 minutes, so user must report to x2345 immediately)

Fermilab implementation

- Two categories of protected PII:
  - Local access only:
    - live in “locked room” major application
    - No downloading or remote access possible
    - Example: neutron therapy
  - Network access required
    - Lives in moderate level major application, behind the MFA firewall; currently only Information Systems Major Application (Peoplesoft, Oracle Financials, and Workday!!)
    - Only certain accounts will be allowed to access the PII portions of these databases, and no access at all from general internet
    - Only special cases (e.g., particle accelerator school) require downloading; these will require waivers and encryption

Enterprise (network access) PII

- For each database containing Protected PII, the specific Protected PII data contained therein will be inventoried and documented
- User accounts are granted access to these systems according to the "least privilege principle". This means that accounts are not granted access to Protected PII data by default.
- Access allowing a user to view any other person's Protected PII data is defined as privileged access. Privileged access is granted only to a documented list of specific users based on demonstrated business need and with management approval.
- A list of specific network segments and addresses will be identified in the associated Major Application plan as being permissible for use for privileged access. These network segments and addresses will have additional security controls applied to the network and computers (MFA!!), defined in the Major Application plan, which enforce restricted access to Protected PII. (not true for Workday, which instead has their own set of security controls)
- Privileged access from network segments or addresses not identified in the MA plan must conform to the Fermilab requirements for remote access to Protected PII (two factor authentication and 30-min inactivity timeout).
- No downloading of protected PII: even on MFA Transfer Disk!

Local (locked room) PII

- Physical controls: Systems and data are physically controlled by remaining in designated restricted access rooms
- Network access controls: These systems will not be connected to the lab general use network. Where the system consists of more than one machine, these machines may be connected together by a dedicated, controlled network, but this network may not interconnect to any other networks at any time, nor will modem or other remote access methods be allowed
- User access controls: System access will be limited to a documented list of user accounts
- No downloading, no access from outside the “locked room”

User Requirements

- All user accounts with access to Protected PII will be granted based on demonstrated business need and with explicit management approval.
- All privileged users granted access to Protected PII will sign a statement agreeing not to download any Protected PII to computer systems or portable media. (Download means moving copies of PII to a local machine or portable media where the PII data persists on the machine or media and would be compromised if the machine or media were stolen or lost). Any reports, extracts, or other data summaries containing Protected PII required by users may only be stored on servers within the Major Application. (Signing the attendance sheet for this training constitutes this agreement)
- All users will be required to attend appropriate training on handling Protected PII.

It’s not just a good idea, it’s the law!

- Whether we like it or not, these regulations come right from the white house and apply to all government information
- Fermilab as part of Dept of Energy is subject to these regulations
- We are being regularly audited to make sure we are in compliance; failure to comply could result in the lab being shut down
- Any users found to be violating policies will lose computing privileges and/or access to site
- Computing systems found in violation will be disconnected and barred from the lab network

Other categories of information

- Responsibility on data owner to categorize and protect data according to general guidelines
- Level 4: Secure Access data: PII and other statute protected data; specific lab wide policies
- Level 3: Restricted Access data: data whose loss or improper disclosure could result in significant harm to the laboratory or to individuals; access restricted to specific identified individuals with business need to know
- Level 2: Limited Access data: data whose loss or disclosure could result in only limited harm; access must be restricted to broad groups of individuals
- Level 1: Open Access data: no restrictions